Modern ICT

Cyberterrorism

Criticality of Civil Aviation
Set of the interconnected components representing informative, personnel and material resources, processes and technologies which are of crucial importance for providing security in the process of gathering, processing, converting, storing and transmitting information in aviation.

For example:
- Flight Management System
- Surveillance Data Distribution equipment
- Controller-Pilot Data Link Communications System
- Surface Movement Radar / Aerodrome Surface Detection Equipment
- Global Distribution System etc.
Potential cause of an unwanted incident, which may result in harm to a system, individual or organization.

ISO/IEC 27032:2012

SINGULARITY:

- Diversity of CAIS` Architecture
- Criticality to Aviation Security
- International Character

©PhD Associate Professor Sergiy Gnatyuk
Main Control Documents

- **Doc 8973** (Guidance on Aviation Security)
- **Doc 9985** (Guidance on the Security of Air Traffic Management System)
- **Doc 30** (ECAC Policy Statement in the Field of Civil Aviation Security)
Recommendation. All Member States must develop security measures for information and communication systems using for civil aviation tasks to protect its against acts of unlawful interference that can make threat to civil aviation.
➢ Security of CAIS and ICT
➢ Cybersecurity of Aviation Infrastructure
➢ Supply Chain Security for Hardware & Software
➢ Cyberattacks & Cyberincidents Recording
Security of ICT
Cybersecurity and CIIP
Security of ATM infrastructure
The appropriate authority should ensure that measures addressing cyber threats to civil aviation have been included in:

- National Civil Aviation Security Programme;
- National Quality Control Programme;
- National Civil Aviation Security Training Programme.
1. CAIS Protection

The appropriate authority should ensure that operators, including air navigation systems providers, airports, air carriers and regulated agents, implement measures to protect Critical Aviation Information Systems.
2. Threat Assessment Process
The appropriate authority should include CAIS in their threat assessment process.
3. Network Separation

The appropriate authority should ensure that networks used for CAIS (for example on board airplane system) should be separated from networks to which the public have access. If separation is not possible, connection and access should be monitored and controlled at all times.
4. Responsibility

The appropriate authority should ensure that responsibility for securing CAIS is allocated by operators to a properly selected, recruited and trained individual. These security measures should be coordinated and consistent with existing aviation security measures.
5. Security by Design
Operators should ensure that security measures are considered in the design, implementation, operation and disposal of new CAIS. Modifications to existing CAIS should take security measures into account to the extent practicable.
6. Supply Chain Security for Hardware and Software

Operators should ensure that reasonable supply chain security measures for hardware and software should be applied to CAIS. The appropriate authority and operators should request details of security measures from potential suppliers when procuring such systems.
7. Remote Access Control

Operators should ensure that remote access to CAIS is only permitted under pre-arranged and secure conditions. The appropriate authority and operators should ensure that suppliers do not have unauthorized access to these systems after they have been procured.
8. Cyber Attack Incident Records

The appropriate authority and operators should record and evaluate incidents of cyber attacks.
Main Problems

- Critical Aviation Information Systems Identifying
- Criticality Assessment of Systems
- AvSec Docs Harmonization with Basic International Standards in Information (Cybernetic) Security
- Development of Methods & Means for Cyberthreats Mitigation Considering its Singularity and Features

©PhD Associate Professor Sergiy Gnatyuk
Sergiy O. Gnatyuk
PhD, Associate Professor
IT-Security Academic Department
National Aviation University (Kyiv, UKRAINE)

Academic Secretary of Dissertation Council D 26.062.17
Scientific Adviser of Engineering Academy of Ukraine
Executive Secretary of Ukrainian Scientific Journal of Information Security (www.infosecurity.nau.edu.ua)
IEEE Member; ICAO Instructor (Cybersecurity in Civil Aviation)

Phones: +380 (97) 193 44 25, +380 (44) 406 70 22
Fax: +380 (44) 406 76 42
E-mail: s.gatyuk@nau.edu.ua
Skype: sergiy.gnatyuk
www.bit.nau.edu.ua

THANK YOU FOR YOUR ATTENTION!